(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平8－305461

(43)公開日　平成８年(1996)11月22日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ　1/00	３７０		Ｇ０６Ｆ　1/00	３７０Ｅ	

審査請求　未請求　請求項の数１　ＯＬ　（全 6 頁）

(21)出願番号　特願平8－107191

(22)出願日　平成８年(1996)４月26日

(31)優先権主張番号　９５３０２８８９．１

(32)優先日　1995年４月28日

(33)優先権主張国　イギリス（ＧＢ）

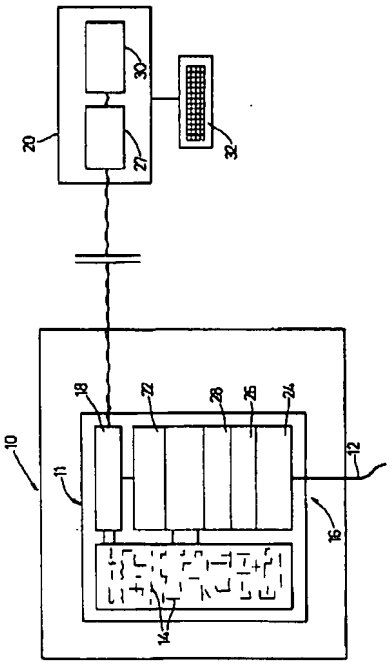
(71)出願人　590000400
ヒューレット・パッカード・カンパニー
アメリカ合衆国カリフォルニア州パロアルト　ハノーバー・ストリート　3000

(72)発明者　グリーム・ジョン・プラウドラ
イギリス国ブリストル　ストーク・ギフォード　タッチストーン・アベニュー　5

(74)代理人　弁理士　上野　英夫

(54)【発明の名称】　セキュリティデバイス

(57)【要約】
【課題】機器が盗難にあった場合等に、その機器を動作不能にする。
【構成】一定周期毎や一定使用回数毎等の所定のタイミングで通信回線経由で認証センタから認証をもらわない限り、機器が正常動作できないようにする。盗難にあった場合には使用者は認証センタに盗難届を出すことにより、認証が出ないようにすることができる。



1

【特許請求の範囲】

【請求項１】装置とともに使用され、セキュリティステーションからの特定の命令信号に応じて前記装置を継続的に動作させるセキュリティデバイスであって、前記セキュリティステーションからの特定の命令信号を受信するための信号受信手段と、認証ルーチン中に前記信号受信手段に応答して、前記特定の命令信号が受信されない場合、前記装置の動作を禁止、阻止、あるいは妨害する中断手段を有するセキュリティデバイス。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は装置に取り付けたり、あるいは内蔵してその装置の盗難を阻止するセキュリティデバイスに関する。

【０００２】

【従来の技術】盗まれた装置を動作不能にして窃盗犯による使用を防止するさまざまな方法が提案されている。カーオーディオシステムの中には、たとえば自動車から一時的あるいは永久的に取り外されたために電源が切れると、あるコードをキー入力するまで適切に動作しないようにする機能を持つものがある。また、遠隔のセキュリティセンタからの命令を受けて付勢される動作阻止器を自動車に取り付ける方法もある。また、遠隔の制御ステーションによって付勢できる不能化ユニットを、テレビ、ビデオテープレコーダ等の電子機器に設ける方法も提案されている。

【０００３】

【目的】しかし、後者のシステムはいずれも動作阻止や動作の不能化を命令する信号を発するための遠隔制御ステーションを必要とし、従って盗まれた装置が遠隔制御ステーションの範囲外に持ち出されたり、遠隔装置との交信が故意にあるいは他のなんらかの理由で不能化されている場合には有効に機能しない。さらに、このようなシステムの安全性は、窃盗犯がある程度の知識を持っていた場合不能化ユニットや阻止器をバイパスすることによって破られることがある。

【０００４】

【概要】本願発明者は、セキュリティデバイスを取り付けた装置が認証ルーチンを周期的に開始させるシステムを考案した。この認証ルーチンが完了するにはセキュリティステーションからのある特定の命令信号を必要とする。

【０００５】従って、本発明の一側面は、装置に取り付けられ、前記セキュリティステーションからのある特定の命令信号によって前記装置を継続的に動作させるセキュリティデバイスであって、前記セキュリティステーションからのある特定の命令信号を受信するための信号受信手段と、認証作業中に前記信号受信手段に応答して前記特定の命令信号が受信されない場合前記装置の動作を禁止、阻止、あるいは中断する中断手段を有するセキュリティデバイスを提供するものである。

2

【０００６】従って、本デバイスでは、所有者がセキュリティステーションに対して装置が盗まれたことを通知した場合、セキュリティステーションは次回の認証作業では適切な命令が送出されず、その結果その後装置が適正に機能しないようにする。また、なんらかの理由で装置が認証作業中に遠隔センタと交信しない場合、装置は適正に機能しない。

【０００７】簡単なシステムでは遠隔センタからセキュリティデバイスへの一方向のみの通信を行なって必要な特定の命令信号を与えるだけしかしないものもある。この場合、認証作業の開始は、おそらくは、装置が警報を発して所有者に電話で遠隔ステーションに連絡を行なうように促すことによって間接的に行なわれる。しかし、セキュリティデバイスに前記セキュリティステーションに前記特定の命令信号を送出するように要求する呼び掛け信号を送出するための信号送出手段を設けることによってこれを自動的に行なうことが好適である。

【０００８】この装置は好ましくは、呼び掛け／応答ルーチンを実装して前記セキュリティステーションから発せられた特定の命令信号が前記呼び掛け信号に対するある特定の応答であるようにし、またセキュリティデバイスに前記特定の応答信号の真偽を判定する手段を備える。

【０００９】この呼び掛け信号と応答信号は、好ましくは、送出時に暗号化し、受信時に解読するようにする。このセキュリティデバイスは、好ましくは、セキュリティデバイスのみが内部的にアクセスして暗号化／解読処理に用いられる１つあるいは複数のキーを記憶できる１回だけ書き込み可能な追記型（WORM）メモリ等のセキュリティメモリ手段を有する。暗号化／解読処理は、公開鍵システムや対称鍵システム等の適当なタイプのうちの任意のものとすることができる。

【００１０】前記セキュリティデバイスと前記セキュリティステーションの間の通信は通信ネットワークを介して行なわれ、前記呼び掛け信号は前記セキュリティデバイスのネットワークアドレスを識別するデータを含み、それによってセキュリティセンタがセキュリティデバイスの論理ロケーションを判定し、そのロケーションに応答信号を送ることができるようにすることが好適である。

【００１１】このセキュリティデバイスは、好ましくは、対象とする装置の制御機能の少なくとも主要な部分を実行する集積回路に組み込むことが好適である。集積回路技術の進歩にともなって、より大規模化するチップにより多くの機能が集積されるようになってきている。本発明の実施例ではこれを利用して、セキュリティデバイスを装置の機能の大部分に相当する回路とともに特定用途集積回路（ASIC）に組み込むようにしている。これによって、このセキュリティデバイスを無力化すること

が実質的に不可能であるというわけではないとしても、少なくとも経済的に実現することはきわめて困難なものとするような安全性が提供される。

【００１２】さらに、たとえば交換用チップの供給を正当な所有者あるいはサービスマンに限定することによって、セキュリティシステムが装置の日常のメンテナンスや修理の妨げとならないようにすることが大いに望ましい。従って、このセキュリティデバイスをASICにしっかりと埋め込んだ場合、交換ASICが簡単に入手できることによってこのシステムの安全性が大きく損なわれてはならない。その理由は、交換ASICもまたその設計上の理由から、適正な機能を達成するために、セキュリティステーションからの定期的な許可が必要だからである。

【００１３】セキュリティデバイスがセキュリティステーションからの命令信号について定期的にチェックするようにするには、色々な方法がある。従って、装置が電源に永久的にあるいは長期間接続される場合、この装置にタイマを設け、タイマがタイムアウトするたびに認証作業を開始することが好適である。これに替えて、あるいはこれに加えて、装置の動作時間が比較的短い場合には、デバイスに装置が動作するか電源投入されるたびにインクリメントする不揮発性カウンタ手段を設けて、このカウンタ手段が所定の数あるいはその倍数に達するたびに認証作業を開始するようにすることができる。

【００１４】セキュリティデバイスとセキュリティステーションの間の通信はさまざまな方法で確立することができる。半固定的に設置されるビデオテープレコーダ等の装置の場合、通信は旧来の電話システム（POTS）を介して行なうことができる。移動する機器や車両用についてのアプリケーションの場合、通信は自動車電話ネットワーク、無線、赤外線データリンク等やその組み合わせを用いて行なうことができ、当業者にはどのような通信システムが適当であるかは明らかであろう。

【００１５】以上の本発明の説明を上に述べたが、本発明は上でまた以下で説明する機能の任意の創作的な組み合わせにも拡張できる。

【００１６】

【発明の実施例】本実施例では、セキュリティデバイス16は導線12によって電源に半永久的に接続されたビデオテープレコーダ（VTR）10に内蔵される。VTR 10はこの装置の機能の大部分が特定用途集積回路（ASIC）11に集積されていることを除けば従来の設計と同じである。従って、このASICはテープとカセットの搬送、選局、プログラミング、計時その他の機械的・電気的機能のほとんどを制御する機能回路要素群14を有しており、VTR 10の商品価値は完全に機能するASIC 11がなければ極めて小さくなる。また、ASIC 11は後に詳細に説明するあるセキュリティ条件が満足されない場合には機能回路要素群14の少なくとも一部の動作を停止させることができるセキュリティデバイス16を含んでいる。この停止は制御に対する応答の一部または全部の禁止、機能回路要素群の一部あるいは全部の出力の不能化といった形態をとることができる。これはたとえば内部信号を休止状態にする、走査波形を除去する、入来した制御信号を休止状態にする、出力を休止状態にする、ある内部回路からクロックあるいは電力を除去する、条件試験入力あるいは割り込み入力を使用してマイクロプロセッサの通常動作を停止する等によって行なうことができる。このような動作は制御信号によってASIC 11内のさまざまな機能回路要素14で起こすことができる。ASIC導体は通常分離が困難であり、これらの導体に電気的接続を行なうことは通常困難である。しかし、本実施例では、これらの導体はASIC 11本体内に埋め込まれ、従ってASIC 11の他の要素を修理不能なほど損傷せずにこのような導体にアクセスすることはできず、これにより安全性を更に向上させている。

【００１７】それぞれがセキュリティ装置内の別々の埋め込みバッファによって駆動される異なる機能回路要素14への許可信号を与える複数の導体があり、これにより“停止”信号をオーバーライドするために複数の接続を行なわなければならない場合がある。それぞれの機能回路要素はセキュリティデバイス16との通信のための通信要素を有し、それぞれの通信要素の動作には単純な論理レベルではなく波形が必要であるようにできる。その結果、複雑性従って妨害に対する免疫性は予見される脅威のレベルに従って選択することができる。

【００１８】説明をわかりやすくするために、機能回路要素群14はセキュリティデバイス16から分離したものとして示されているが、実際にはこれらの回路要素は、上述したよう、セキュリティデバイス16の動作が不能化される可能性を最小限にするように入り交じるようにさせる。

【００１９】セキュリティデバイス16は適当な任意の通信媒体（ここではPOTSシステム）で遠隔セキュリティセンタ20との間で信号の送受信を行なうことのできるトランシーバ18を有する。トランシーバ18はここではASIC 11上にあるように示されているが、これはASIC 11とは別に設けることもできる。また、セキュリティデバイス16は暗号技術に基づく呼び掛け／応答法を実行し、それに関する暗号化データを記憶するための回路22を有する。このような暗号化システムは周知である。たとえば、John Wiley and Sons刊のDavies、Price著“Security for Computer networks”1989年第２版の“Peer Entity Authentication”やISO 9798“Peer Entity Authentication Mechanism Using An n-bit Secret Key”を参照されたい。呼び掛け／応答機構にはさまざまなものがある。その複雑さの程度もさまざまであるが、基本的にはセキュリティデバイス16が乱数を得て、それを第１のキーK1を用いて暗号化し、遠隔セキュリティセンタ20に送出できるものとなっている。これが呼び掛けである。遠隔セ

キュリティセンタ20はキーK1を用いてこの呼び掛けを解読し、それを第２のキーK2を用いて暗号化し、セキュリティデバイスに送り返す。これが応答である。セキュリティデバイスはキーK2を用いてこの応答を解読し、解読された数がもとの乱数と同じであるかどうかをチェックする。これによってセキュリティデバイスに対してそのメッセージがキーK1およびK2の知識を持つ遠隔セキュリティセンタ20と考えられるエンティティから来たものであることが証明される。遠隔セキュリティセンタ20はセキュリティデバイス16が動作の継続を許可されている場合にのみ応答を与える。従って、公開鍵、対称鍵等の暗号化システムを用いることができる。

【００２０】また、セキュリティデバイス16はASIC 11の電源投入を検出する電源投入検出回路24、タイマ26および不揮発性カウンタ28を有する。ASIC 11は１回だけ書き込み可能な追記型メモリ（WORM）を有する。これは、好ましくは溶断可能リンク式デバイスであるが、不透明パッケージに入ったEPROMとすることもできる。

【００２１】遠隔セキュリティセンタ20はある領域内で多数の装置に対応することができ、POTSシステムを介してASIC 11を内蔵した装置との間で信号の送受信を行なうためのトランシーバ27を有する。また、遠隔セキュリティセンタ20は暗号技術を実装しまた関係する暗号化データを記憶するための回路30と、オペレータがある選択された装置が盗難にあったものと識別されたときその装置への応答信号の送出を防止するためのオペレータインターフェース32を有する。

【００２２】このシステムの動作に当たっては、工場出荷時に、ASIC 11は好ましくはWORM内のキー対を用いてプログラムされ、対応するキー対が遠隔セキュリティセンタ20を運営する中央局に登録される。図２には、認証のための動作の中の個々の装置内で必要な動作を実行する許可チップの動作のフローチャートを示す。ここにおいて、フローチャート中の各ブロックの動作は以下のようになっている：

１３８：スイッチが入る

１４０：不揮発性カウンタをインクリメントする［外部からは書込めない］

１４２：カウンタの値がチェックポイントに来ていることを示しているか？

１４６：権限をチェックする

１５０：外部認証装置ＯＫか？

１４８：通常動作を停止し、手動の「権限チェック」の開始を待つ

１５２：内部の不揮発性タイマがチェックポイントに来ていることを示しているか？

１５４：通常動作を行う（タイマは動作している）

１４４：不揮発性タイマとカウンタをリセットする

図２に示すように、VTR 10がオンされると、不揮発性カウンタ28がインクリメントされ、デバイスはこのカウンタが所定の数あるいはその倍数に達しているかどうかを判定する（ステップ140、142）。

【００２３】カウンタ28が前記数かその倍数に達している場合、デバイスは遠隔セキュリティセンタ20を呼び出し、呼び掛けを発し、上述した暗号化および解読のステップを用いて応答を要求することによって認証作業を開始する。遠隔セキュリティセンタ20に対して、VTR 10が盗まれたとの報知が行なわれていなければ、センタは応答を返し、この応答がセキュリティデバイス16によって予測された通りのものであるかどうかがチェックされ、予測通りであれば、デバイスはVTR 10の動作を継続させる。次に、タイマ26とタイマ28がステップ44でリセットされ、デバイスはタイムドルーチン46に入る。

【００２４】VTR 10が通信媒体から切り離されている場合、あるいは遠隔セキュリティセンタ20が応答を送出しないように警報を受けている場合、応答が受け取られないことによってステップ48においてセキュリティデバイス16がトリガされ、上述した中断技術のうちの一つを用いてVTR 10の通常動作が停止され、認証作業のマニュアル起動を待つ状態になる。

【００２５】電源投入検出時にカウンタ28があらかじめ設定された数に達しない場合、カウンタ28はタイムドルーチン46に入る。ここで、タイマ26はタイムアウトになるまで作動し、タイムアウトになると、セキュリティデバイス16は遠隔センタ20を呼び出すことによって認証作業を開始する。

【００２６】正当な所有者がセキュリティデバイス16を内蔵した装置の盗難に気づくと、所有者はただちに遠隔セキュリティセンタ20を運営する局を呼び出し、この局は適切なチェックを行なった後、盗まれた装置にいかなる応答信号も送らないように、遠隔セキュリティセンタに命令する。従って、この装置は、適切な通信媒体に接続されていたとしても、応答信号が着信しないことによってセキュリティデバイスがトリガされると動作不能になり、その商品価値はきわめて小さくなる。

【００２７】このシステムの変更態様として、セキュリティデバイス16から発せられる呼び掛けには、セキュリティデバイスの出所ネットワークアドレス（POTSを介して通信が行なわれる場合ユーザの電話番号）等のユーザのアイデンティティあるいはロケーションを表わすデータを含めることができる。遠隔セキュリティセンタ２０は、意図的な通信の中断の後にこの同じネットワークアドレスに応答を返す。これによって、遠隔セキュリティセンタ２０はセキュリティデバイス16の論理ロケーションをモニタすることができ、また場合によっては追跡機能が付与される。

【００２８】以下に、本発明の実施態様の例を列挙する。

【００２９】［実施態様１］装置とともに使用され、セキュリティステーションからの特定の命令信号に応じて

前記装置を継続的に動作させるセキュリティデバイスであって、前記セキュリティステーションからの特定の命令信号を受信するための信号受信手段と、認証ルーチン中に前記信号受信手段に応答して、前記特定の命令信号が受信されない場合、前記装置の動作を禁止、阻止、あるいは妨害する中断手段を有するセキュリティデバイス。

【００３０】［実施態様２］前記セキュリティデバイスは前記セキュリティステーションに前記特定の命令信号の送出を要求する呼び掛け信号を送出するための信号送出手段を有することを特徴とする実施態様１記載のセキュリティデバイス。

【００３１】［実施態様３］前記セキュリティデバイスと前記セキュリティステーションは通信ネットワークを介して通信し、前記呼び掛け信号は前記セキュリティデバイスのネットワークアドレスを識別するデータを含むことを特徴とする実施態様１に記載のセキュリティデバイス。

【００３２】［実施態様４］前記セキュリティステーションからの前記特定の命令信号は前記呼び掛け信号に対する特定の応答信号を含み、前記セキュリティデバイスは前記特定の応答信号を確認する手段を有することを特徴とする実施態様１ないし３の何れかに記載のセキュリティデバイス。

【００３３】［実施態様５］前記呼び掛け信号を暗号化する手段を有することを特徴とする実施態様４記載のセキュリティデバイス。

【００３４】［実施態様６］前記特定の応答は暗号化された形態であり、前記デバイスは前記特定の応答を解読する手段を有することを特徴とする実施態様４または実施態様５記載のセキュリティデバイス。

【００３５】［実施態様７］前記暗号化処理のための１つあるいは複数のキーを記憶するためのセキュリティメモリを有することを特徴とする実施態様５または実施態様６記載のセキュリティデバイス。

【００３６】［実施態様８］前記中断手段は装置の制御機能を実行する回路を含む集積回路に組み込まれることを特徴とする実施態様１ないし７の何れかに記載のセキュリティデバイス。

【００３７】［実施態様９］前記集積回路は装置の制御機能の少なくとも主要部分を含むことを特徴とする実施態様８記載のセキュリティデバイス。

【００３８】［実施態様１０］タイムアウトになると前記認証ルーチンを起動するタイマー手段を有することを特徴とする実施態様１ないし９の何れかに記載のセキュリティデバイス。

【００３９】［実施態様11］前記装置の電源投入を検出する電源投入検出手段と、電源投入のたびにインクリメントされ、カウント値が所定の数あるいはその倍数に達すると前記認証ルーチンを起動させる不揮発性カウンタ手段を含むことを特徴とする実施態様１ないし１０の何れかに記載のセキュリティデバイス。

【図面の簡単な説明】

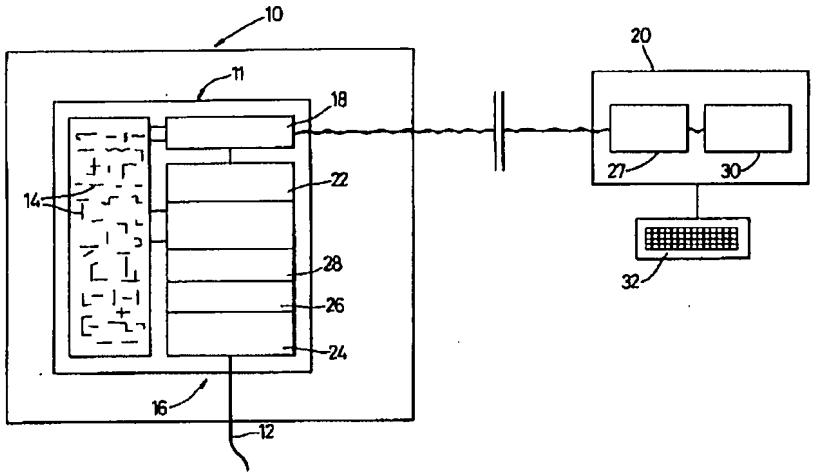
【図１】本発明のセキュリティデバイスの一実施例を取り付けた装置の概略図。

【図２】図１のセキュリティデバイスの動作を示すフローチャート。

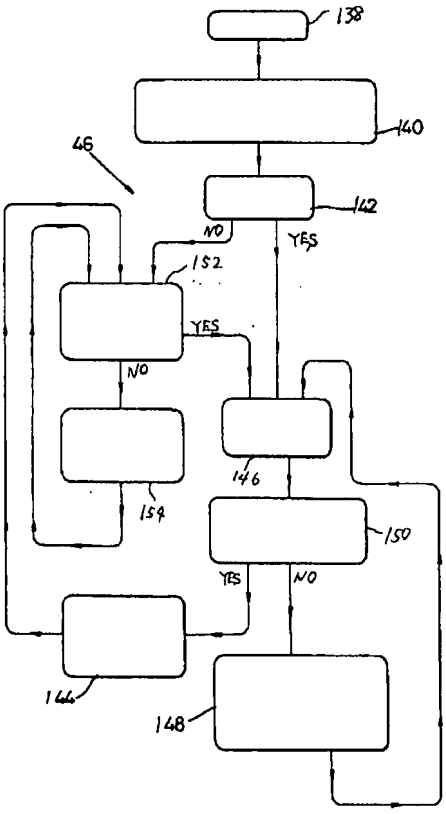
【符号の説明】

10：ビデオテープレコーダ（VTR）
11：特定用途集積回路（ASIC）
12：導線
14：機能回路要素群
16：セキュリティデバイス
18：トランシーバ
20：遠隔セキュリティセンタ
22：回路
24：電源投入検出回路
26：タイマ
27：トランシーバ
28：不揮発性カウンタ
30：回路
32：オペレータインターフェース
46：タイムドルーチン
K1：第１のキー
K2：第２のキー

【図１】


10
11
18
20
22
14
27
30
28
26
24
32
16
12

【図２】


138
140
46
142
NO
YES
152
YES
NO
146
154
150
YES
NO
144
148